**IT Applications  
Tammy**

**Unit 4, Outcome 2  
Ch 8 Security Measures  
Security Equipment**

**Hardware**

**Biometrics**

1. What is biometrics?  
   Biometrics is the use of physical human characteristics, like fingerprints or facial features or behavioural characteristics such as voice patterns or handwriting, to grant access to data.
2. From the following list of biometric devices, note their strengths and weaknesses.

**Swipe Cards**

1. For what purpose are swipe cards used for?  
   Used for electronic transactions and also internal security within an organisation.
2. What is the limitation of a swipe card?  
   Limitation of the swipe card is that it can be easily damaged by magnetic fields.

**Smart Cards**

1. What is the difference between a smart card and a swipe card?  
   The difference between the smart card and swipe card is that the smart card has a microchip embedded into it to store and manipulate data.

**Security Tokens**

1. Why is this known as two factor authentication?  
   It’s known as a two factor authentication as it needs a name and password to access it.
2. What are the advantages of this method?  
   It cannot be accessed even if lost.

**Power Protection**

1. List the power protection devices

* Surge protector
* Spikes
* Uninterruptible power supply

**Avoiding System Failure**

1. List the two main safeguards against system failure

* Redundancy through multiple hard drives or fault-tolerant equipment
* Redundancy through mirror server

1. What does the term redundancy mean in this context?  
   Redundancy means that no single part of the system is critical to its overall operation. If one part fails the others can take over its job and keep the system running until it is replaced.
2. How does mirroring drives work?
3. Describe RAID technology
4. What is the major difference between a mirror computer and RAID technology?

**Backup Media**

1. List the considerations to be taken into account before deciding on which backup device.

* Cost of drive
* Cost of media per megabyte (MB) or gigabyte (GB)
* Speed
* Compatibility

**Magnetic Media:**

List the characteristics of the following media types;

1. **Floppy disk drive**

* Simplest to use for small back-up jobs
* Can be easily damaged
* 1.44mb capacity
* Are not used any more

1. **Super disk drive**

* Similar to floppy disk
* Can store 120mb

1. **Jaz drive**

* Popular with multimedia artists
* Removable cartridges can hold up to 2GB

1. **Hard disk drive**

* Affordable option to back up files onto a second hard drive

1. **Magnetic tape**

* Cheap but are slow
* They have to be accessed sequentially

**Optical Drives**  
List the characteristics of the following media types;

1. **CD-ROM**

* Can hold up 700MB of data
* Comes as either CD-R ( can only be used once) or CD-RW (can write data to disc couple of times).

1. **DVD**

* Can store up to 9GB of data
* Same as the CD the DVD can either be used once (DVD-R) or can be used many times (DVD-RW)

**Solid-state Drives**  
List the characteristics of the following media types;

1. USB storage devices, whatare the benefits of these drives?

* Small
* Can be taken anywhere
* No moving parts
* Hold up to 2GB data

**Online Backups**

1. Describe the nature of this type of backup?  
   Data is backed up to a remote server via the Internet to data centres that have fault-tolerant servers, redundant power supplies and uninterruptible power supplies.
2. What is an enterprise storage system  
   Interconnection via a storage area network, of RAID discs, tapes, CD/DVD-ROM servers, internet backup and any other networked storage devices.
3. List the advantages of this type of backup

**Surveillance technology to protect the security of information**

**Packet Sniffers**

1. Describe how these work and what do they monitor  
   Packet sniffers are diagnostic tools that monitor the contents of packets of data being sent across networks. They can be set to filter packets containing certain data elements and copy them to an administrator’s computer for further analysis.

**Desktop Monitoring Programs**

1. Describe the nature of these programs and who are fond of these applications  
   Desktop monitoring programs work by intercepting every single action that’s performed on a computer. These programs allow an employer to see what is on your desktop, even to the point of watching what you are typing.

**Log Files**

1. What are log files?  
   Log files are records of the sites that you have visited that are stored in a cache.

**Closed Circuit Television (CCTV)**

1. For what purpose are they used  
   They are used so they can see what is happening in the workplace. This can reduce theft, violation and vandalism.

**Telephones**

1. How can these occur?

**Audit Trails**

1. What is the purpose of audit trial and list what is included in an audit trail.  
   Audit trial is used to trace transactions or any other form of activity in a system. They include log files of system login, both successful and unsuccessful, any other files accessed, modified or copied.

**Physical security devices**

1. List these devices.

* Lockable disc box
* Safe
* Security cables

**Encryption**

1. Describe how encryption works?  
   It disguises the contents of the message, it becomes meaningless jumble. It can only be read by the intended recipient.

**Network Policies and Procedures**

1. List the nature of network policies and procedures

* Enter username and password to log on

1. What makes a good password?  
   Good password would be something that you can remember like a cat or dogs name, however it isn’t an ideal password as it is to simple. A good password should contain numbers and letters and be at least 6 characters in length

**Firewalls**

1. Explain the role of firewall?  
   Firewalls block users from outside the network getting in.

**Anti-virus Software**

1. How does this software work?  
   Prevents a computer from getting virus or infections.
2. What is a virus signature?